Software Engineering Institute

CERT Resilience Management Model—Mail-Specific Process Areas: Mail Revenue Assurance (Version 1.0)

Julia H. Allen
Gregory Crabb (United States Postal Inspection Service)
Pamela D. Curtis
Nader Mehravari
David W. White (formerly with the SEI)

August 2014

TECHNICAL NOTE
CMU/SEI-2014-TN-011

CERT Division

http://www.sei.cmu.edu

Carnegie Mellon

This material is based upon work funded and supported by USPS under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of USPS or the United States Department of Defense.

This report was prepared for the
SEI Administrative Agent
AFLCMC/PZM
20 Schilling Circle, Bldg. 1305, 3rd floor
Hanscom AFB, MA 01731-2125

DM-0001550

Table of Contents

Abstract iii

Introduction 1

Mail Revenue Assurance 3

Purpose 3

Outline 3

Introductory Notes 4

Related Process Areas 8

Summary of Specific Goals and Practices 9

Specific Practices by Goal 9

MRA:SG2 Prepare for Managing Mail Revenue Risks 14

MRA:SG3 Assure Mail Revenue 17

MRA:SG4 Manage Mail Revenue Risks 27

Mail Revenue Assurance Process Area References 31

References 31

Abstract

Developing and implementing measurable methodologies for improving the security and resilience of a national postal sector directly contribute to protecting public and postal personnel, assets, and revenues. Such methodologies also contribute to the security and resilience of the mode of transport used to carry mail and the protection of the global mail supply chain. Since 2011, the U.S. Postal Inspection Service (USPIS) has collaborated with the CERT® Division at Carnegie Mellon University's Software Engineering Institute (SEI) to improve the resilience of selected U.S. Postal Service (USPS) products and services. The CERT Resilience Management Model (CERT-RMM) and its companion diagnostic methods served as the foundational tool for this collaboration.

This report includes one result of the USPIS/CERT collaboration. It is an extension of CERT-RMM to include a new mail-specific process area for revenue assurance. The purpose is to ensure that the USPS is compensated for all mail that is accepted, transported, and delivered.

Introduction

In December 2011, the U.S. Postal Inspection Service (USPIS) asked CERT staff to develop new mail-specific process areas (PAs) to manage the resilience of mail throughout its lifecycle—from induction to delivery. The initial scope of this effort included mail acceptance, revenue confirmation, mail security, mail transport, and mail custody.

The CERT® Resilience Management Model (CERT-RMM) [Caralli 2011], which was developed by the CERT Division at Carnegie Mellon University's Software Engineering Institute (SEI), and its companion diagnostic methods served as the foundational tool for this collaboration. CERT-RMM is a capability-focused maturity model for improving an organization's management of operational resilience activities across the domains of security management, business continuity management, and aspects of information technology operations management. These improvements enable high-value services to meet their missions consistently and with high quality, particularly during times of stress and disruption.

The USPIS objectives for this project included the following [Crabb 2012, Joch 2013]:

- Define common criteria for assuring that U.S. Postal Service (USPS) products are resilient.
- Evaluate business partners and customer operations in their handling of mail.
- Use these new PAs in conjunction with other selected CERT-RMM PAs to evaluate new and existing USPS products, services, suppliers, and partners, in terms of their security and resilience.
- Assure that each product's contribution to USPS revenue is commensurate with services delivered.
- Identify revenue collection gaps more quickly.

The development project commenced in January 2012 and was an active collaboration between USPIS subject matter experts and CERT staff. The architecture of the mail-specific PAs follows that of the existing 26 PAs described in CERT-RMM. The scope and content of these PAs evolved significantly during the course of the development project. In July 2012, initial outlines for four mail-specific PAs—Mail Induction (MI), Mail Revenue Assurance (MRA), Mail Transportation (MT), and Mail Delivery (MD)—were accepted by the USPIS, as well as an initial draft of the MRA PA.

The PAs specific to the induction of mail and to mail revenue assurance were pilot tested extensively during the Express Mail projects described in an SEI technical note titled *Improving the Security and Resilience of U.S. Postal Service Mail Products and Services Using the CERT® Resilience Management Model* [Crabb 2014]. In April 2013, outlines for all four

® CERT is a registered mark of Carnegie Mellon University.

mail-specific PAs were accepted as baselined by the USPIS, and in July 2013, baselined versions of two complete PAs, MI [Allen 2014b] and MRA, were accepted by the USPIS. Following this initial effort, the USPIS asked CERT to extend the goals and practices contained within the MT outline for U.S. domestic mail to address international mail transportation. This effort is described in the report titled *CERT Resilience Management Model Mail-Specific Process Areas: International Mail Transportation, Version 1.0* [Allen 2014a].

The Mail Revenue Assurance Process Area is presented in this report.

Mail Revenue Assurance

Purpose

The purpose of Mail Revenue Assurance (MRA) is to ensure that the USPS is compensated for all mail that is accepted, transported, and delivered.

Outline

MRA:SG1 Satisfy Standards Governing Mail Revenue

Mail standards, policies, operating procedures, and other specifications related to and affecting mail revenue are satisfied for each type of mail service.

MRA:SG1.SP1 Establish Standards Governing Mail Revenue

Standards, policies, operating procedures, and other specifications governing mail revenue are established and maintained for each type of mail service.

MRA:SG1.SP2 Establish Controls for Satisfying Standards Governing Mail Revenue

Controls are established and maintained to satisfy standards, policies, operating procedures, and other specifications related to and affecting mail revenue.

MRA:SG1.SP3 Address Inconsistencies Between Standards Governing Mail Revenue and Controls Established to Satisfy Standards

Inconsistencies between standards governing mail revenue and the controls established to satisfy them are identified and addressed.

MRA:SG2 Prepare for Managing Mail Revenue Risks

Preparation for managing mail revenue risks is performed.

MRA:SG2.SP1 Determine Mail Revenue Risk Sources and Categories

The sources of risk to mail revenue are identified and the categories of risk that are relevant to mail revenue are determined.

MRA:SG2.SP2 Establish a Mail Revenue Risk Management Strategy

A strategy for managing mail revenue risk is established and maintained.

MRA:SG3 Assure Mail Revenue

Payment to USPS is assured for every mailpiece that is accepted, transported, and delivered.

MRA:SG3.SP1 Verify that Postage Affixed Is Sufficient

Affixed postage is verified to represent sufficient postage for the purchased mail service in accordance with standards governing mail revenue.

MRA:SG3.SP2 Verify that Postage Is Not Fraudulent

Postage is verified as not fraudulent in accordance with standards governing mail revenue.

MRA:SG3.SP3 Verify Receipt of Payment for Mail

Mail revenue is verified as paid to USPS.

MRA:SG3.SP4 Address Mail Revenue Discrepancies

Discrepancies in the verification of postage affixed and discrepancies related to fraudulent postage are identified and addressed.

MRA:SG3.SP5 Investigate Fraudulent Postage, Postage Affixed, and Forms of Payment

Mailpieces with fraudulent postage, postage affixed, or forms of payment are identified and mailpiece information is collected for further investigation.

MRA:SG4 Manage Mail Revenue Risks

Operational risks to the assurance of mail revenue are identified and addressed.

MRA:SG4.SP1 Identify and Assess Mail Revenue Risks

Operational risks to mail revenue are periodically identified and assessed.

MRA:SG4.SP2 Address Mail Revenue Risks

Identified operational risks to mail revenue are addressed.

Introductory Notes

This CERT Resilience Management Model (CERT-RMM) mail-specific process area describes key goals and practices that will be used as a standalone evaluation tool or in conjunction with other CERT-RMM process areas to evaluate the extent to which the USPS receives revenue for all mailpieces that it accepts, transports, and delivers.

The viability of the USPS and its ability to meet its mail service commitments to its customers rely on being correctly, accurately, and adequately compensated for each piece of mail that it accepts, transports, and delivers. First class mail volume has been decreasing steadily since 2001 due to the increasing use of email and the internet for correspondence and business transactions. Organizations such as Federal Express (FedEx) and the United Parcel Service (UPS) directly compete with the USPS for the delivery of urgent letters and parcels. Lower mail volume means lower revenues to support the legal USPS commitment to deliver mail to every address, currently six days per week. To respond to this current state, the USPS has increased their level of automation, optimized and re-optimized postal routes, and consolidated facilities. Despite these measures, the USPS continues to experience budget shortfalls, which makes its ability to assure revenue even more critical [Wikipedia, 30 May 2013].

Mail revenue is determined based on the purchased mail services, which reflect mailpiece class, type, and extra services. As described in the Mail Induction process area MI:SG2.SP2, Accept Mail, mailers (those who submit mail to the USPS) are responsible for proper payment of postage. Postage on all mail must be fully prepaid or paid at the time of mailing, except as specifically provided by the USPS Domestic Mail Manual (DMM) [DMM 606.6.1, pg. 1119]. USPS mail acceptance personnel (and supporting mail acceptance and processing

equipment and systems) verify payment to ensure that mail is inducted according to standards governing mail revenue and to ensure that payment is made according to the range of requirements associated with specific mailers and mailings. Acceptance personnel assist mailers with establishing payment accounts and transacting payment for business mailings [DAR, pg. 4]. The handling of mail with insufficient, incorrect, or fraudulent payment is treated as a discrepancy as described in MRA:SG3.SP4, Address Mail Revenue Discrepancies.

Mailers must comply with all applicable USPS standards in paying for mail services. The types of postage that appear on each mailpiece are the basis for identifying and collecting revenue. Types of postage include [POM 442, p 276; Mehravari 2013]

- stamps
- prepaid stationery and packaging (such as stamped envelopes and prepaid priority mail flat rate envelopes)
- postage evidencing systems (such as APC [automated postal center] and PVI [postage validation imprinter] postage as well as customer meter and PC postage products)
- permit imprints

Standards for prices for types and classes of mail and standards for types of postage are described in the DMM.

Postage may include indicia. Indicia are comprised of human-readable information and machine-readable information. Accepted postage indicia must be legible (readable by USPS personnel and mail acceptance and processing equipment and systems). There are particular data associated with different types of indicia, depending on the purchased mail services. Indicia may include postage related to the class of mail, presort level,[1] and extra service endorsements. Illegible or unreadable (unscannable) indicia are not acceptable as payment of postage [DMM, pg. 1105]. Standards for affixing postage and verifying that postage is sufficient and not fraudulent are defined in the DMM [604.4.3.3, .4, pg. 1106].

Types of Postage

Stamps

One type of postage is *stamps*. Stamps are typically a small piece of paper that is affixed to a mailpiece, providing evidence of postage payment for that mailpiece. Unless excepted by standard and unless purchased by the USPS, the total postage reflected by the stamp that is affixed must be equal to or greater than the postage charge for the purchased mail service [DMM 604.1.2, pg. 1092]. Stamps that are precanceled may also be affixed to mailpieces.

[1] Presort is the process by which a mailer prepares mail so that it is sorted to at least the finest extent required by the standards for the price claimed. Generally, presort is performed sequentially, from the lowest (finest) level to the highest level, to those destinations specified by standard and is completed at each level before the next level is prepared [DMM 235.1.1, pg. 209].

Precanceling is the cancellation of adhesive postage, stamped envelopes, or stamped cards before mailing. Precanceling may be done by the mailer under a postal permit or mailers may purchase precanceled stamps bearing a price category from the USPS. Precanceled stamps are specifically for presorted first-class mail and standard mailpieces [DMM 604.3.1.5, pg. 1097]. Postmasters should ensure that sufficient security is provided for the stamp stock at the physical site where stamps are sold and stored [POM 225.65, pg. 192].

Prepaid Stationery and Packaging

A second type of postage is prepaid stationery and packaging, which includes stamped stationery (stamped envelopes, stamped cards, and aerogrammes) and prepaid packaging (prepaid priority mail flat rate envelopes and prepaid forever priority mail flat rate packaging).

Postage Evidencing Systems

A third type of postage is a broad category called postage evidencing systems (PES). PES includes the following USPS operated retail postage evidencing systems:

- APC stamps and labels
- PVI postage strips, with and without barcodes
- metering systems
  - customer digital meters, with and without information-based indicia (IBI[2]) barcodes
  - PC postage products such as Click-N-Ship and authorized third-party suppliers such as endicia.com, stamps.com, Pitney Bowes, and eBay

A postage evidencing system is a device (such as a postage meter) or system of components a mailer uses to print evidence that postage required for mailing has been paid. Postage evidencing systems print indicia, such as IBI, to indicate postage payment. Mailers print indicia directly on a mailpiece or on a label that is affixed to a mailpiece [DMM 604.4.1, pg. 1101]. PC (personal computer) postage products are one form of postage evidencing system that allow mailers to purchase and print postage with IBI directly onto mailpieces, shipping labels, and USPS-approved customized labels. Examples include stamps.com, Click-N-Ship, and endicia.com.

Postal-owned postage meters are restricted items that must be handled securely in accordance with Handbook AS-701 Material Management. This meter equipment must not be assigned to contract stations, branches, or community post offices. Contractors may rent a postage meter at their own expense, however, subject to the same rules and regulations that apply to private mailers [POM 142.12, pg. 129].

---

[2] Information-based indicia: a secure postage evidencing standard used by the USPS to indicate electronic postage payment. IBI is a two-dimensional PDF417 or data matrix barcode combined with human-readable information. The barcode data contains such information as amount of postage, origin Zip Code, destination, mail class, weight, confirmation/tracking numbers, and a cryptographic signature. The human-readable information shows at a minimum the information required by the USPS DMM [Wikipedia, 16 Mar 2012].

Mailers must enter into an agreement with the USPS for authorization to use postage evidencing systems. By entering into the agreement, a mailer accepts responsibility for control and use of the system and agrees to abide by all rules and regulations governing its use [DMM 604.4.2.1, pg. 1103].

Metering systems are devices that allow the download, storage, and accounting of postage in the device. Metering systems print indicia that may be IBI or non-IBI, to indicate postage payment. IBI is digitally generated. The machine-readable information that is contained in IBI identifies the postage evidencing system, postage payment information, and mail service requested [DMM 604.4.3.4, pg. 1106]. USPS-approved IBI postage meters electronically transmit transactional data to the USPS.

Permit Imprint

A fourth form of postage is a *permit* imprint (indicia) advance deposit account established with the USPS. Standards for permit imprint mailings and payment for this type of mailing are described in the DMM [604.5, pg. 1111]. Each mailpiece sent under this payment method must bear a permit imprint indicia showing that postage is paid. A mailer may obtain a permit to use a permit imprint indicia and pay postage in cash before or at the time of mailing. Payment must be made for each mailing, either in cash or through an advance deposit account, before the mailing is accepted. All mailpieces in a permit imprint mailing must meet the standards specified in the DMM for the price claimed. Mail must be deposited, verified (including payment), and accepted at the post office that issued the permit, at a time and place designated by the postmaster. Exceptions to this include plant-verified drop shipments, where mail is accepted at the destination USPS facilities and combined mailings (such as from the large presorters), where permit imprint mail from one post office can be accepted at the post office where the combined mailer has their permit imprint. Mailers must have a separate account (permit) in each location where they present mail [DAR, pg. 4; more detail is available in DAR 2.3, pg. 10].

For mailings that require a postage statement (mail paid with a permit imprint [DMM, pp. 86, 97, 111, 186]), the mailer certifies compliance with all applicable standards governing mail revenue when signing the corresponding postage statement [DMM 607.1, pg. 1141].

A permit imprint, bulk, or other discount price mailing (for example, see plant-verified drop shipments below) is accepted after an examination of the mailing and the accompanying postage statement prepared by the mailer. A USPS employee's signature on the postage statement and the subsequent acceptance of the mailing do not constitute verified accuracy of that statement and do not limit the ability of the USPS to demand proper payment after acceptance when it becomes apparent such payment was not made [DMM 607.1, pg. 1141].

Plant-Verified Drop Shipments and Plant Load Mailings

Plant-verified drop shipments (PVDS) enable origin verification and postage payment for shipments transported by a mailer (or third party) at the mailer's expense, on the mailer's

own or contracted vehicle, to destination USPS facilities for acceptance as mail [DMM 705.16, pg. 1393]. PVDS mail is eligible for entry discounts.

Plant-load mailings consist of mail from one mailer or the combined mailings of two or more mailers loaded into one or more USPS transportation vehicles and accepted by the USPS at the mailers' plants when [POM 461.43, pg. 289]

1. a single postage statement is prepared and submitted by the mailers if required for each mailing;
2. proper postage is affixed to each item (not fraudulent; postage affixed is verified); or
3. an alternative method of paying postage using a permit imprint (e.g., manifest mailing) is used, and a single postage statement and a manifest covering the mailing are prepared and submitted by the mailer.

Plant-load mailings are not eligible for entry discounts.

All PVDS and plant-load mailings must be verified and postage and fees must be collected in accordance with DMM and POM standards, Handbook DM-109, *Business Mail Acceptance,* and Handbook DM-103, *Official Mail* [POM 464.1, pg. 295]. Plant-load mailings are typically submitted to a Detached Mail Unit (DMU) or a Business Mail Entry Unit (BMEU). Under an expedited plant-load shipment authorization, the USPS verifies the mail for presort and postage at the mailer's plant, and postage is calculated from and paid at the post office where the mailer is authorized to plant load [POM 461.2, pg. 289].

Mail revenue assurance as described in this process area relies upon the ability of the USPS and its supporting investigative service, the United States Postal Inspection Service (USPIS), to identify and satisfy standards governing mail revenue (MRA:SG1); prepare to manage mail revenue risks (MRA:SG2); verify that postage affixed is sufficient, that postage is not fraudulent, and receipt of payment (MRA:SG3); handle mail revenue discrepancies and investigate fraudulent postage and payment (MRA:SG3); and effectively manage mail revenue risk (MRA:SG4).

Related Process Areas

The acceptance of mail and the handling of mailpieces are addressed in the Mail Induction process area.

The processing and transportation of mail is addressed in the Mail Transportation Process Area.

The processing and delivery of mail is addressed in the Mail Delivery process area.

Compliance with mail revenue standards for mail and mail postage is addressed in the Compliance process area.

The management of the internal control system that assures mail revenue is addressed in the Controls Management process area.

Instances of uncollected revenue and revenue fraud are identified as events in MRA:SG3, Assure Mail Revenue. The analysis of such events, their declaration as incidents, and the appropriate USPS response are addressed in the Incident Management and Control process area.

The monitoring and control of the satisfaction of standards governing mail revenue are performed in the Monitoring process area.

The risk management cycle for mail revenue risks is addressed in the Risk Management process area.

Summary of Specific Goals and Practices

MRA:SG1 Satisfy Standards Governing Mail Revenue
- MRA:SG1.SP1 Establish Standards Governing Mail Revenue
- MRA:SG1.SP2 Establish Controls for Satisfying Standards Governing Mail Revenue
- MRA:SG1.SP3 Address Inconsistencies Between Standards Governing Mail Revenue and Controls Established to Satisfy Standards

MRA:SG2 Prepare for Managing Mail Revenue Risks
- MRA:SG2.SP1 Determine Mail Revenue Risk Sources and Categories
- MRA:SG2.SP2 Establish a Mail Revenue Risk Management Strategy

MRA:SG3 Assure Mail Revenue
- MRA:SG3.SP1 Verify that Postage Affixed Is Sufficient
- MRA:SG3.SP2 Verify that Postage Is Not Fraudulent
- MRA:SG3.SP3 Verify Receipt of Payment for Mail
- MRA:SG3.SP4 Address Mail Revenue Discrepancies
- MRA:SG3.SP5 Investigate Fraudulent Postage, Postage Affixed, and Forms of Payment

MRA:SG4 Manage Mail Revenue Risks
- MRA:SG4.SP1 Identify and Assess Mail Revenue Risks
- MRA:SG4.SP2 Address Mail Revenue Risks

Specific Practices by Goal

MRA:SG1 Satisfy Standards Governing Mail Revenue

Mail standards, policies, operating procedures, and other specifications related to and affecting mail revenue are satisfied for each type of mail service.

Standards, policies, operating procedures, and other relevant specifications for the identification and collection of mail revenue are essential for ensuring that the USPS is properly and adequately compensated for every mailpiece that it accepts and delivers. Such standards permit the USPS to assure that all mailers that present mail for acceptance, transportation, and delivery have fulfilled their payment obligations.

MRA:SG1.SP1 Establish Standards Governing Mail Revenue

Standards, policies, operating procedures, and other specifications governing mal revenue are established and maintained for each type of mail service.

Standards, policies, operating procedures, and other specifications governing mail revenue (standards for short) for mail services and postage are specified in the DMM and maintained by the USPS Mailing Standards Department (refer to MI:SG1.SP2 for additional information). The DMM defines standards for prices, eligibility, and postage payment methods for all classes and types of retail mail and retail mail services. The DMM also defines standards for prices, eligibility, and postage payment and documentation for all classes and types of commercial (business) mail and commercial mail services. To qualify for USPS business mail prices, mailers are required to prepare mailings in accordance with specific DMM mail preparation and postage standards [DAR, pg. 7].

Standards governing mail revenue establish the requirements that the USPS imposes on all mailers that submit mailpieces to the USPS for delivery. The standards reflect requirements that are necessary to help ensure the financial viability of the mail-handling process and the USPS. However, while the USPS proposes standards governing mail revenue (including rates), these must be approved by the Postal Regulatory Commission. Standards reflect affiliations that may impose additional standards and restrictions (such as the acceptance of international mail), agreements with external entities (mailers of various types), and external requirements that are imposed by U.S. laws and regulations.

The conditions under which the USPS operates are constantly changing. As a result, the requirements for financial viability and ensuring that the USPS is correctly, accurately, and adequately compensated for all mail that it handles continue to evolve as well. The USPS must be adept at recognizing changes in conditions that precipitate considerations for changes in standards governing mail revenue.

Managing changes to standards governing mail revenue involves several distinct criteria:

- identifying change triggers and criteria such as the addition of a new postal product
- identifying mail services and types of postage that may be affected by these triggers
- assessing the impact of changes on standards
- identifying and documenting changes to existing standards (or identifying new standards, if necessary)
- communicating changes to standards to those responsible for their enforcement (mail acceptance personnel) and implementation (mailers)
- identifying mail scanning, processing, and other equipment and systems (including postage evidencing systems) that must be changed as a results of changes to standards

Compliance obligations that may result in or form the basis for standards governing mail revenue are identified and managed in the Compliance process area.

Typical Work Products

1. Standards governing mail revenue for mail services
2. Standards for stamps
3. Standards for prepaid stationery and packaging

4. Standards for postage evidencing systems
5. Standards for permit imprints
6. Change requests to standards

Subpractices

1. Identify standards governing mail revenue for mail services.
2. Identify standards governing mail revenue for postage.
3. Communicate standards to all affected parties (USPS personnel, acceptance offices, mailers).
4. Develop and publish new standards as needed to reflect changes in revenue assurance practices.
5. Follow established procedures for revising existing standards.
6. Document approved revisions to existing standards in all affected publications, including cross-references in the POM to the DMM.
7. Communicate changes to standards to all affected parties (USPS personnel, acceptance offices, mailers).
8. Make standards available to mailers, USPS personnel, and other users of the standards in appropriate locations and formats.
9. Ensure that USPS personnel use standards to verify that mailers adhere to standards.

MRA:SG1.SP2 Establish Controls for Satisfying Standards Governing Mail Revenue

Controls are established and maintained to satisfy standards, policies, operating procedures, and other specifications related to and affecting mail revenue.

A control is a policy, procedure, method, technology, or tool that satisfies a stated objective. For satisfying standards, policies, operating procedures, and other specifications that relate to and affect mail revenue, focus on the subset of controls that demonstrate the satisfaction of such standards, provide confidence that they are being followed, and reduce the risks to the USPS of receiving insufficient compensation for the mail services it provides.

Controls can be broad or specific. Broad controls typically apply universally to all processes that can affect mail revenue, for example, ensuring that accurate and current agreements with meter vendors and certain PC postage vendors are in effect for adhering to the CFR (Code of Federal Regulations) and that vendors are regularly reviewed for compliance with such regulations. Another example is data-based controls used for sampling and reconciliation. Such controls support trend analysis as well as analysis of patterns of behavior to identify discrepancies and potential fraud. Specific controls are applied to mail products (such as Priority Mail Express and Click-N-Ship) and also include in-process controls that happen at specific points in the mail stream lifecycle, for example, the use of scanning systems to detect the use of counterfeit stamps.

Controls can be administrative, technical, or physical. Administrative controls ensure alignment to USPS management's intentions and include such actions as governance, setting policy, monitoring, auditing, and performance measurement. Technical controls are implemented through technology means. They typically exist in automated processes, manifested in software, hardware, devices, systems, and networks. Examples include functions within the Electronic Verification System (e-VS) to monitor and check for shortpaid mail, functions within the Advanced Facer Canceler System to detect counterfeit and cancelled stamps, and fraudulent postage detection methods such as detectors and devices for

- luminescent indicia
- luminescent material in the ink on meter stamps
- phosphorus coating a postage stamp
- scanning and determining the legitimacy of IBI
- functions within Delivery Bar Code Sorter (DBCS) systems and Automated Parcel Processing Systems (APPS) for identifying duplicate IBIs

Physical controls provide physical barriers to access that typically apply to people and facilities such as picture IDs, card readers, and locks. Examples of physical controls for standards governing mail revenue may include restricted access to mail acceptance areas to minimize the induction of bypass mail.

The subpractices included in this practice are generically addressed in the Controls Management process area.

Typical Work Products

1. Mail revenue controls (including the responsible party)
2. Traceability matrix of standards, policies, operating procedures, and other specifications and controls
3. Mail revenue control gaps
4. Mail revenue control updates

Subpractices

1. Establish controls to satisfy standards governing mail revenue.

   These can be a combination of controls that already exist, controls that have to be updated, and new controls that have to be implemented.

2. Confirm or assign responsibility for implementing controls.

   Confirmation is required for existing and updated controls. Assignment is required for new controls.

3. Develop a bidirectional traceability matrix that maps standards and controls.

4. For standards that are not addressed by controls, either address control gaps or identify and manage the risks associated with control gaps as described in MRA:SG4, Manage Mail Revenue Risk.

5. Regularly review, assess the effectiveness of, and update or retire controls.

MRA:SG1.SP3 Address Inconsistencies Between Standards Governing Mail Revenue and Controls Established to Satisfy Standards

Inconsistencies between standards governing mail revenue and the controls established to satisfy them are identified and addressed.

USPS acceptance personnel and mailers make commitments to perform activities and implement controls that are consistent with standards governing mail revenue and that ensure the satisfaction of those standards. They also make commitments to ensure that standards are reflected in mail acceptance and processing equipment and systems to the extent applicable. This specific practice aims to ensure that acceptance personnel and mailers are capable and prepared to meet the standards to which they have made commitments (whether or not they are under the direct control of the USPS).

The analysis of standards governing mail revenue is performed to identify conflicts between the standards and the controls established to satisfy the standards, specifically where controls makes it difficult or impossible to assure that mail revenue has been identified and collected. Based on the complexity of the mail lifecycle (acceptance to delivery) and all of the parties that contribute to the handling of mail, it is likely that the intent of any specific standard for any mail services and for any form of postage may not always be realized.

Because standards governing mail revenue derive from more than one source, it is possible that acceptance personnel and mailers in good faith commit to standards but in reality are constrained in satisfying them. Identifying these inconsistencies proactively can help the USPS resolve conflicts, take mitigating actions (such as implementing compensating controls), and negotiate with participating parties to make changes or grant exceptions to standards as needed.

The monitoring and control of the satisfaction of standards governing mail revenue is performed in the Monitoring process area.

Compliance with standards governing mail revenue for mail services and postage is performed in the Compliance process area.

(Refer to the Controls Management process area, specifically CTRL:SG4.SP1, for further information about periodically assessing and adjusting controls.)

Typical Work Products

1. Documentation of inconsistencies

2. Corrective actions

Subpractices

1. Review the planned or implemented controls for consistency with standards governing mail revenue. Identify any changes made to the standards.

2. For USPS acceptance personnel
   - Document constraints that may impede satisfaction of standards.
   - Identify changes that have to be made to controls (or planned controls) to ensure satisfaction of standards as specified.
   - Initiate corrective actions to enforce alignment between standards and controls.

3. For mailers
   - Document constraints that may impede satisfaction of standards
   - Identify changes that have to be made in controls (or planned controls) to ensure satisfaction of standards as specified.
   - Initiate corrective actions to enforce alignment between standards and controls.

4. For mail acceptance and processing equipment and systems
   - Document constraints that may impede satisfaction of standards.
   - Identify changes that have to be made in controls (or planned controls) to ensure satisfaction of standards as specified.
   - Initiate corrective actions to enforce alignment between standards and controls.

MRA:SG2 Prepare for Managing Mail Revenue Risks

Preparation for managing mail revenue risks is performed.

Preparation for managing mail revenue risks requires the USPS to develop and maintain a strategy for identifying, analyzing, and addressing risks to mail revenue. This strategy is documented in a risk management plan and describes the activities that the USPS performs to carry out a continuous mail revenue risk management program. This includes identifying the sources and types of risk and establishing a strategy that details the USPS approach, activities, and objectives for managing those risks.

MRA:SG2.SP1 Determine Mail Revenue Risk Sources and Categories

The sources of risk to mail revenue are identified and the categories of risk that are relevant to mail revenue are determined.

Identifying risk sources helps the USPS determine and categorize the types of mail revenue risk that are most likely to affect the USPS's ability to receive compensation for all mail that it accepts, transports, and delivers. In addition, identifying risk sources helps in developing a USPS-specific risk taxonomy that can be used as a tool for managing mal revenue risk on a continuous basis as operating conditions, mail products, and mail systems change and evolve. The sources of risk can be both internal and external to the USPS.

Categorizing mail revenue risks provides a means by which the USPS can perform advanced analysis and mitigation activities that allow for similar types of risks to be effectively neutralized or contained.

Typical Work Products

1. List of mail revenue risk sources
2. List of mail revenue risk categories
3. Mail revenue risk taxonomy

Subpractices

1. Determine sources of mail revenue risk.

   Risk sources are fundamental areas of risk that can affect the USPS's ability to identify and collect payment for mail services. Risk sources represent common areas where risks may originate. Typical internal and external sources of mail revenue risk include [Mehravari 2013]

   - counterfeited, duplicated, falsified, photoshopped, or otherwise modified postage
   - insufficient (shortpaid) postage
   - unpaid (bypass) postage
   - unreadable information-based indicia (IBI)
   - reused and duplicated IBI and intelligent mail barcodes (IMBs)
   - bad forms of payment including bad checks, credit cards, and Automated Clearing House (ACH) accounts (illegitimate accounts and insufficient funds)
   - theft of payment account numbers
   - theft of user ids and passwords for online payment accounts as well as counterfeit online accounts
   - meter tampering
   - fraudulent schemes by dishonest mailers
   - postage statement and manifest errors
   - vulnerabilities in technologies that support the assurance of mail revenue

   Approaches for determining risk sources include

   - structured brainstorming on types of postage and types of payment
   - conducting interviews and workshops with subject matter experts (SMEs)
   - reviewing past investigations, case histories, and audit results
   - reviewing vendor irregularity reports
   - reviewing verification failures (such as those reported by MERLIN)

   Defining risk sources in advance provides a means for early identification of risk and can inform actions that need to be taken to address risks that can cover a broad array of risks to mail revenue before the USPS realizes the consequences of these risks.

2. Determine categories of mail revenue risk.

   Risk categories provide a means for collecting and organizing risk for ease of analysis and mitigation. Typical categories align with the various sources of mail revenue risk and may include risks resulting from insufficient affixed postage, fraudulent postage, and fraudulent forms of payment. Risks to mail revenue may also align with types of mail services, specific mailers, specific geographic locations or regions, specific types of postage, and specific types of postage payment.

   Approaches for determining risk categories include performing affinity grouping of risk sources, conducting SME interviews and working groups, and reviewing investigation results.

3. Create a mail revenue risk taxonomy.

   A mail revenue risk taxonomy is a way to collect and catalog common revenue risks that the USPS is subject to and must manage. The risk taxonomy is a means of communicating these risks and for developing USPS-specific actions if mail revenue is affected by them.

MRA:SG2.SP2 Establish a Mail Revenue Risk Management Strategy

A strategy for managing mail revenue risk is established and maintained.

Because of the pervasive nature of mail revenue risk, a comprehensive risk management strategy is needed to ensure proper consideration of such risks and the effects on the USPS's ability to receive compensation for mail services. The strategy provides a common foundation for the performance of mail revenue risk activities (which are typically dispersed throughout the USPS) and for the collection, coordination, and elevation of mail revenue risk to the USPS's enterprise risk management process.

Typical items addressed in a mail revenue risk management strategy include

- the scope of mail revenue risk management activities
- the methods to be used for risk identification, analysis, mitigation, monitoring, and communication
- the sources of mail revenue risk
- how the sources of risk should be organized, categorized, compared, and consolidated
- parameters for measuring and taking action on mail revenue risks
- techniques to be used for addressing risk such as the development of new controls and updates to existing controls
- definition of risk measures to monitor the status of mail revenue risks
- time intervals for risk monitoring and reassessment
- staff involved in mail revenue risk management and the extent of their involvement in the activities noted above

The mail revenue risk management strategy should be developed to facilitate the accumulation of relevant risks as input to the USPS's enterprise risk management strategy

and program. The strategy should be documented and communicated to all relevant stakeholders, internal and external, that are responsible for any mail revenue risk management activity.

Typical Work Products

1. Mail revenue risk management strategy

Subpractices

1. Develop and document a mail revenue risk management strategy that aligns with the USPS's overall enterprise risk management strategy.
2. Communicate the mail revenue risk management strategy to relevant stakeholders and obtain their commitment to the activities described in the strategy.

MRA:SG3 Assure Mail Revenue

Payment to USPS is assured for every mailpiece that is accepted, transported, and delivered.

The assurance of mail revenue is accomplished by ensuring that adequate controls are in place to verify that postage affixed is sufficient, verify that postage is not fraudulent, and verify receipt of payment. Each mailpiece that is accepted by the USPS during induction (refer to the Mail Induction process area), transportation (refer to the Mail Transportation process area), and delivery (refer to the Mail Delivery process area) is required to have verified, affixed postage and postage that is not fraudulent for the purchased mail service. According to standards governing mail revenue, all postage must be prepaid at the time of mail acceptance. It is, therefore, the responsibility of mail acceptance personnel (supported by mail acceptance and processing equipment and systems) to verify that sufficient funds have been paid or are available in applicable accounts to assure that the USPS receives the revenue to which it is entitled for the mail services it provides.

Additionally, the assurance of mail revenue is accomplished by ensuring that adequate controls are in place to identify and handle discrepancies concerning mail revenue. Examples of discrepancies include fraudulent postage, insufficient affixed postage for the purchased mail service, and insufficient funds on account to pay for a submitted mailing. Controls for investigating fraudulent postage, insufficient affixed postage, and fraudulent forms of payment such as counterfeit or duplicated postage are required to minimize the likelihood that the USPS accepts mail for which it will not be paid.

MRA:SG3.SP1 Verify that Postage Affixed Is Sufficient

Affixed postage is verified to represent sufficient postage for the purchased mail service in accordance with standards governing mail revenue.

Each mailpiece that is accepted by the USPS is required to have postage affixed in a specified and defined manner that is *sufficient* for the purchased mail service for that mailpiece (as contrasted with *not fraudulent*, which is described in MRA:SG3.SP2). Required mail postage is described in the DMM. To the extent possible, acceptance personnel (and supporting equipment and systems) located at the various acceptance sites are responsible

for verifying that the mailpieces and affixed postage presented to them meet standards governing mail revenue for the prices claimed [DAR, pg. 7].

The value of affixed postage on each mailpiece must be equal to or greater than the amount due for the applicable service and any extra service fees, or another amount permitted by standards [DMM 604.4.3, pg. 1104].

The purpose of this specific practice is to ensure that adequate controls have been established and are being maintained to verify that affixed postage is sufficient. Adequate controls to verify affixed postage provide confidence that the USPS is receiving or will receive the revenue to which it is entitled for the mail services it provides for each mailpiece.

Attributes of a mailpiece for the purpose of determining and verifying affixed postage include weight, postal zone, shape, and dimensions. Attributes of a commercial mail submission to an acceptance facility for the purposes of determining affixed postage include accuracy of postage statements, historical mailpiece volume, volume of mailpieces for a specific shipment, presort levels, extent of automation, and systems used to submit and pay for mailpieces.

These are some examples of controls that are required to verify affixed postage:

- permit imprint: verify that the accompanying postage statement is valid (corresponds to a legitimate, active, funded permit); verify that the postage statement is accurate (provides a correct count of all mailpieces, their attributes, and their purchased mail services)
- metering systems: verify affixed postage for the purchased mail services and attributes
- stamps: verify affixed postage for the purchased mail services and attributes
- permit imprint, presorted metered, and precanceled stamps: compare the postage statement to the mailer's supporting documentation, which can include a *Qualification Report and a Summary Zip Destination Report*

Revenue deficiency means a shortage or underpayment of postage or fees. Mailpieces bearing insufficient (shortpaid) postage are those for which the total postage and fees affixed are less than the postage required for the applicable services and any extra services fees. Mailpieces bearing unpaid postage are those for which the mailer has not paid the postage or additional fees due to the lack of affixed postage, the use of counterfeited, duplicated, falsified, otherwise modified postage, or postage with zero value [DMM 604.4.4, pg. 1106]. For mailpieces with shortpaid or unpaid postage found in the mail stream, manual and automated processes are used to detect and verify the revenue deficiencies [DMM 604.4.4, p 1107]. Mail that is received at either the office of mailing or office of address without enough postage is marked to show the total deficiency of postage and fees [DMM, 604.8.1, pg. 1121].

Verification of postage in the mail acceptance process is addressed in the Mail Induction process area, specifically MI:SG2.SP2, Accept Mail.

Mailpieces with shortpaid or unpaid postage that does not sufficiently reflect the purchased mail services and attributes of the mailpiece are handled as discrepancies, as described in MRA:SG3.SP4 Address Mail Revenue Discrepancies. The investigation of mailpieces with affixed postage that is not sufficient is addressed in MRA:SG3.SP5, Investigate Fraudulent Postage, Postage Affixed, and Forms of Payment.

The identification and mitigation of mail revenue risks that may result from shortpaid or unpaid postage are addressed in MRA:SG3 Manage Mail Revenue Risk and in the Risk Management process area.

Typical Work Products

1. Affixed postage control gaps and updates
2. Affixed postage discrepancies

Subpractices

1. Analyze existing affixed postage controls against standards governing mail revenue.

   Ensure that existing controls are adequate to identify affixed postage that is not sufficient and any related discrepancies. Examples of such controls include

   - manual inspection
   - verification that a specific postage statement accurately reflects the submitted mailing and that funds are available in the mailer's account
   - the use of postage scanning systems (such as the Advanced Facer Canceler System (AFCS), DBCS, APPS, and Passive Adaptive Scanning System (PASS); scans from some of these systems are imported into the Total Revenue Protection (TRP) system for further analysis)
2. Identify control gaps and proposed updates.
3. Refer affixed postage discrepancies for further handling.

MRA:SG3.SP2 Verify that Postage Is Not Fraudulent

Postage is verified as not fraudulent in accordance with standards governing mail revenue.

Each mailpiece that is accepted by the USPS is required to have postage that is *not fraudulent* for the purchased mail service for that mailpiece (as contrasted with *sufficient*, which is described in MRA:SG3.SP1). Required postage is described in the DMM. To the extent possible, acceptance personnel (and supporting equipment and systems) located at the various acceptance sites are responsible for verifying that the mailpieces and affixed postage presented to them meet standards governing mail revenue [DAR, pg. 7].

The purpose of this specific practice is to ensure that adequate controls have been established and are being maintained to verify that postage is not fraudulent. The purpose of such controls is to provide confidence that postage conforms to established standards

governing mail revenue and, where required, can be traced to authorized mailers. This increases the likelihood that the USPS will be adequately compensated for each mailpiece that is accepted (refer to MRA:SG3.SP1, Verify that Postage Affixed Is Sufficient). Establishing controls to verify that postage is not fraudulent is the first step to ensure that the USPS will receive the revenue to which it is entitled for the mail services it provides.

Postage includes (but is not limited to) stamps (including precanceled stamps), prepaid stationery and packaging, postage evidencing systems (including metering systems), and permit imprints. Metering systems include customer meters and PC postage products that may contain postage with IBI. Some of the information contained in IBI postage and barcodes may be used to identify and collect mail revenue. An IMB [DAR, pg. 5] may also be affixed to a mailpiece. The information contained in IMBs can be scanned and attached to a specific postage statement and a specific authorized mailer. As a result, an IMB may be used to identify, collect, and assure mail revenue. Depending on the mail services, postage must reflect the following attributes of the mailpiece to which they are affixed: weight and postal zone, and, where applicable, shape and dimensions.

These are some examples of controls that are required to verify that postage is not fraudulent:

- permit imprint: verify that postage is not fraudulent and that each mailpiece can be traced to a specific and authorized mailer
- metering systems: verify that postage is not fraudulent and that each mailpiece can be traced to a specific and authorized mailer
- stamps: verify stamps are not fraudulent and that the stamp is canceled so that it cannot be reused

Verification of postage in the mail acceptance process is addressed in the Mail Induction process area, specifically MI:SG2.SP2, Accept Mail.

Mailpieces with fraudulent postage are handled as discrepancies, as described in MRA:SG3.SP4, Address Mail Revenue Discrepancies. The investigation of mailpieces with fraudulent postage is addressed in MRA:SG3.SP5, Investigate Fraudulent Postage, Postage Affixed, and Forms of Payment.

The identification and mitigation of mail revenue risks that may result from fraudulent postage are addressed in MRA:SG4, Manage Mail Revenue Risk, and in the Risk Management process area.

Typical Work Products

1. Fraudulent postage control gaps and updates
2. Fraudulent postage discrepancies

Subpractices

1. Analyze existing controls to identify fraudulent postage against standards governing mail revenue.

Ensure that existing controls are adequate to identify fraudulent postage and any related discrepancies. Examples of such controls could include

- manual inspection
- verification that a specific postage statement is not associated with a specific and authorized mailer or is associated with a fraudulent mailer
- the use of postage scanning systems (such as the AFCS, DBCS, APPS, and PASS; scans from some of these systems are imported into the TRP system for further analysis)

2. Identify control gaps and proposed updates.
3. Refer fraudulent postage discrepancies for further handling.

MRA:SG3.SP3 Verify Receipt of Payment for Mail

Mail revenue is verified as paid to USPS.

According to standards governing mail revenue, payment of postage for all mailpieces is due at the time they are submitted to acceptance personnel. As described in MRA:SG3.SP1 and MRA:SG3.SP2, postage payment due to the USPS is determined by

- verifying that affixed postage is sufficient
- verifying that postage is not fraudulent
- for permit mail, submitting accurate and valid postage statements (and other supporting documentation such as manifests) associated with a mailing

The purpose of this specific practice is to ensure that adequate controls have been established and are being maintained to verify that revenue for all accepted mailpieces is collected in a timely manner (i.e., prepaid or at the time of the acceptance of mailpieces) and verified as collected. Adequate controls to verify that revenue has been collected provide confidence that the USPS is receiving the revenue to which it is entitled for the mail services it provides for each mailpiece.

Mail payment options vary by mailer and postage payment method. Payment options may also vary by the type of product used for meter imprints, such as PC postage and other evidencing systems [DMM 604.4.3, pg. 1104].

These are some examples of payment methods that mailers may choose to use:

- Stamps: pay for and affix stamps and precanceled stamps to mailpieces
- Metering systems: pay for and affix meter postage to mailpieces
  - accounts in the Computerized Meter Resetting System (CMRS), sometimes referred to as an Additional Postage account
- Permit imprint (a complete postage statement must accompany each mailing paid with a permit imprint): affix permit postage to mailpieces
  - precanceled stamps, which may also use an Additional Postage account to pay for additional postage
  - advance deposit account

- for Priority Mail Express: USPS Corporate Account ACH, Centralized Account Payment System (CAPS), credit card)

Stamps (including purchased precanceled stamps) and meter postage produced by metering systems are paid for prior to being affixed to a mailpiece, so no additional verification is required other than ensuring that postage has not been reused (for example, all stamps have been canceled). Verifying that meter postage has not been reused or duplicated is a much more challenging form of verification and is not yet fully performed.[3]

For permit mail (including precanceled stamps that are purchased with a permit), acceptance personnel (supported by equipment and systems) are required to perform verification procedures and collect the proper amount of postage for all mailings. Personnel must review the mailer's account to verify that the permit number[4] on mailpieces matches the postage statement, that appropriate fees (such as the annual presort fee) have been paid, and that sufficient funds are available [Handbook DM-109, pp. 12, 34].

Induction and verification of postage for plant-loaded mail is described in the POM [464, pg. 295]. The mailer must pay postage and fees for plant-loaded mail to the post office that issued the permit to the mailer (origin post office) before the vehicle is transported from the mailer's plant, except under POM 464 and current DMM policy [POM 464.4, pg. 298]. All *expedited* plant-load shipment mailings must be verified and have postage and fees collected according to the purchased mail services as required in Handbook DM-109 and Handbook DM-103 before it is loaded into mailer-supplied transportation and dispatched [POM 467.4, pg. 304].

Receipt of payment for Priority Mail Express is also verified on delivery. This is an additional control in the event that payment was missed on acceptance.

A significant category of unpaid commercial (business) mail is *bypass* mail. Bypass mail enters the USPS mailstream without the acceptance office (typically a BMEU) recording the transaction, resulting in unrecognized (uncollected) revenue. Bypass mailings may occur due to procedural breakdowns, mail volume in excess of capacity, time-sensitive mailings that must be processed, or fraudulent activity. Bypass mailings may occur in the following circumstances [Handbook DM-109 2-7.1, pg. 24]:

---

[3] Additional verifications for presorted metered and presorted precanceled stamp mailings can be performed. These mailings are verified to determine how much additional postage is owed the USPS or in the case of a Value-Added Refund mailing, how much the USPS must refund for a metered mailing. In addition, the Performance Based Verification (PBV) module of PostalOne! can call for a series of verifications to be performed on any discount mailing. These verifications are generally only performed when called for by PBV [Stephens 2013].

[4] A permit number is not always on the mailpiece, for example, in a company style permit imprint. Downstream from the acceptance office, these types of permits make it difficult to verify payment [Stephens 2013].

- Permit imprint mail is deposited at unauthorized postal sites (e.g., contract postal units or collection boxes) where it is collected. The mail is inducted into the USPS mailstream and the revenue is not recognized.
- Mail may be inadvertently transported to an acceptance facility for processing without being verified by acceptance personnel (for example, no Hold/Staged tags or clearance forms are visible or mail is submitted to an unauthorized area) and the postage statements are not recorded; therefore the revenue is not recognized.
- Mail is directly inducted into operations without the acceptance facility's knowledge due to fraudulent activity (refer to MRA:SG3.SP5).

Once bypass mail is detected, acceptance personnel must contact the affected parties (for example, the mailer, the facility manager, the postmaster, etc.) and must log the occurrence on a bypass mail log for further handling. Logged occurrences of bypass mail means that the USPS captured and recorded the bypass mail event. Obviously of greater concern is bypass mail that is not captured, resulting in nonpayment for a mailing.

Mailpieces for which sufficient postage payment cannot be collected and mailpieces for which payment of postage cannot be verified are handled as discrepancies, as described in MRA:SG3.SP4, Address Mail Revenue Discrepancies. Instances of lack of payment for mailpieces where revenue fraud is the objective are addressed in MRA:SG3.SP5, Investigate Fraudulent Postage, Postage Affixed, and Forms of Payment. There may be instances where lack of payment is first considered a discrepancy and then escalated to fraud.

The identification and mitigation of mail revenue risks that may result from insufficient postage payment are addressed in MRA:SG4, Manage Mail Revenue Risk, and in the Risk Management process area.

Typical Work Products

1. Postage payment control gaps and updates
2. Postage verification control gaps and updates
3. Identified discrepancies to postage payment
4. Identified fraudulent postage payments

Subpractices

1. Analyze existing postage payment controls against standards governing mail revenue.

   Ensure that existing controls are adequate to
   - collect postage
   - verify that postage has been paid
   - identify discrepancies to postage payment
   - identify fraudulent postage payment

   Examples of such controls are
   - manual inspection

- verification that a specific postage statement accurately reflects the submitted mailing and that funds are available in the mailer's account
- the use of postage systems (such as *PostalOne!*, the AFCS, DBCS, APPS, and PASS

2. Identify control gaps and proposed updates.
3. Refer discrepancies to postage payment for further handling.
4. Refer fraudulent postage payment for further handling.

MRA:SG3.SP4 Address Mail Revenue Discrepancies

Discrepancies in the verification of postage affixed and discrepancies related to fraudulent postage are identified and addressed.

Revenue discrepancies are identified as events. The USPS must be able to monitor and identify revenue discrepancy events as they occur, as well as to determine when an event or a series of events constitutes an incident that requires further handling and escalation (a coordinated and planned response). Failure to properly identify events in a timely manner can shift the USPS management burden from effective revenue collection to revenue loss, which can be much more costly.

In order to apply incident management processes, the USPS must have a foundational structure for event detection, reporting, logging, and tracking, and for collecting and storing event evidence. *The processes for effectively performing these practices are described in IMC:SG2, Detect Events.*

The following categories of discrepancies are addressed in this specific practice:

- shortpaid or unpaid postage (discrepancies related to verifying that affixed postage is sufficient as described in MRA:SG3.SP1)
- missing or invalid postage (discrepancies related to fraudulent postage as described in MRA:SG3.SP2)
- postage payment that is not collected or not verified as collected (as described in MRA:SG3.SP3)
- bypass mail that was submitted by mistake or missed (fraud is not the motive)
- refunds

The following sections provide examples of actions that may be taken to handle specific types of revenue events and incidents.

For verified shortpaid or unpaid postage, corrective measures may include [DMM 604.4.4, pg. 1107]

- delivering the mailpiece to the addressee and collecting the deficient revenue as postage due. Such mail that is refused by the addressee or otherwise undeliverable is returned to the sender (for payment and possible redelivery) or treated as dead.

- collecting the deficient revenue from the sender prior to further dispatch and delivery as described in the DMM
- returning the mailpiece to the sender [DMM, pg. 1107]

Upon verification of a revenue deficiency with metering system IBI postage, the USPS electronically notifies both the mailer and the metering system service provider of the revenue deficiency and delivers the mailpiece to the addressee. The notification provides a link to the web-based customer payment portal that permits the mailer to pay or dispute the revenue deficiency [DMM, pg. 1107]. A resolution process is provided through the web-based customer payment portal. The mailer must make payment within 14 days from the date the USPS sends the electronic notification by accessing the web-based customer payment portal or choosing another method identified in the notification. Any mailer disputes regarding the revenue deficiency must be made during this 14-day period. The metering system service provider may be notified to temporarily suspend the mailer's account [DMM, pg. 1107]. The disputes and appeals process is defined in the DMM.

For refunds, corrective measures may include the following:

- In general, a full refund may be made when the USPS is at fault, when postage or fees are paid in excess of the lawful prices, and if postage and retail or extra service fees are paid and no service is rendered [DMM 604.9.2.1, 604.9.2.4].
- For postage evidencing systems and metered postage, refunds may be requested for unused indicia, unused postage value remaining in a postage evidencing system, and the unused balance in a postage payment account [DMM 604.9.2.1].
- For Priority Mail Express, the USPS refunds the postage for an item not available for customer pickup at the destination or for which delivery to the addressee was not attempted, subject to the standards for this service [DMM 113.4.2.6].

Additional examples of cases where refunds may be paid are described in the DMM.

The analysis of revenue discrepancy *events*, their declaration as incidents, and the appropriate USPS response are addressed in the Incident Management and Control process area.

Typical Work Products

1. Revenue discrepancy events

Subpractices

1. Detect and report revenue discrepancy events (as described in IMC:SG2, Detect Events).

MRA:SG3.SP5 Investigate Fraudulent Postage, Postage Affixed, and Forms of Payment

Mailpieces with fraudulent postage, postage affixed, or forms of payment are identified and mailpiece information is collected for further investigation.

Occurrences of mail revenue fraud resulting from fraudulent postage, fraudulent postage affixed, and fraudulent forms of payment are identified as events. The USPS must be able to

monitor and identify revenue fraud events as they occur, as well as determine when an event or a series of events constitutes an incident that requires further handling and escalation (a coordinated and planned response). Failure to properly identify events in a timely manner can shift the USPS management burden from effective revenue collection to revenue loss, which can be much more costly.

In order to apply incident management processes, the USPS must have a foundational structure for event detection, reporting, logging, and tracking, and for collecting and storing event evidence. The processes for effectively performing these practices are described in IMC:SG2 Detect Events.

The following categories of revenue fraud are addressed in this specific practice [DMM 604.4.4, pg. 1106]:

- shortpaid or unpaid postage (fraud related to insufficient affixed postage as described in MRA:SG3.SP1)
- counterfeited, duplicated, falsified, or otherwise modified postage . This may include counterfeit stamps, permit imprints, and metering systems (fraudulent postage as described in MRA:SG3.SP2)
- fraudulent postage statements
- fraudulent postage payment accounts
- bypass mail where fraud is identified as the motive

Additional examples of mail revenue fraud are as follows:[5]

- Permit imprint mail: Mailing is entered into the system without first being properly verified.
- Presorted (discount) mail: Mailing does not qualify for the rates claimed. The mailer submitted more mail than claimed or claimed refunds for higher volumes than what was entered in the mailstream.
- Plant-verified drop shipments: Mailer adds mailpieces after the mailing is verified. The mailer states that a container of mail was left out of a shipment and has already been paid for when in fact it's additional mail.
- Eligibility fraud: Mailing does not meet requirements for the rate claimed or does not have a valid authorization for preferential rates, such as for periodicals or nonprofit mail.
- Bribery, collusion, or employee misconduct: Mailer or postal employee colludes with a mailing representative to avoid postage payments.
- Metering systems: Mailer counterfeits meter indicia or manipulates meters to avoid paying postage.
- IBI: Mailer counterfeits indicia or reuses IBI postage.

[5] https://postalinspectors.uspis.gov/radDocs/revenuefraud/RevenueRisks.html

- Retail fraud: Mailer uses a fraudulent credit card or a bad check to purchase postal products or services.
- Stamp counterfeits: Mailer uses counterfeit stamps.
- Customer fraud: Third-party mailers charge customers for services not provided, which may give customers the impression that the USPS failed to provide the requested service.

Examples of actions that may be taken to handle mail revenue fraud events and incidents are as follows:

- Counterfeit stamps must be confiscated and sent to the postal inspector in charge of the district where the post office is located. A receipt identifying the stamps must be given to persons from whom counterfeit stamps are confiscated [POM 132.42, pg. 106].
- Postage evidencing systems and other online customer payment postage methods generate labels that may be photocopied, manipulated, or modified. Any mailpiece identified as bearing a photocopied or duplicated label should be refused at the retail window or during carrier pickup at a residence or business. Local management should be advised when a photocopied or duplicate label has been identified. Local management may contact the USPIS if additional guidance is needed [POM 136.6, pg. 109].
- Mailpieces bearing IBI postage that are shortpaid (the postage is insufficient for the weight) and where the amount of postage paid is not visible should be marked "returned for postage" and returned to the sender.

All parties who suspect revenue fraud should contact the USPIS.

The analysis of mail revenue fraud events, their declaration as incidents, and the appropriate USPS response are addressed in the Incident Management and Control process area.

Typical Work Products

1. Mail revenue fraud events

Subpractices

1. Detect and report mail revenue fraud events (as described in IMC:SG2, Detect Events).

MRA:SG4 Manage Mail Revenue Risks

Operational risks to the assurance of mail revenue are identified and addressed.

The management of operational risks to mail revenue is the specific application of risk management tools, techniques, and methods to assure that the USPS is adequately compensated for all mail that is accepted, transported, and delivered by the USPS. Due to the high volume of mail, the variety of postage, the extensive geography over which it is delivered, and the number of organizations and individuals that participate in the mail process, there are many opportunities for mail revenue risks to be realized. Revenue risks to

mailpieces can affect the financial viability of the USPS and thus its ability to provide mail services.

Managing mail revenue risks involves ensuring that controls are adequate to identify all occurrences of mailpieces with postage that is not fraudulent, sufficient affixed postage, and sufficient payment of postage and ensuring that the USPS is compensated for these mailpieces. Managing mail revenue risks also involves ensuring controls are adequate to identify all occurrences of mailpieces with fraudulent postage, insufficient affixed postage, and insufficient payment of postage. Both categories of risk are most likely to occur during the mail acceptance process as described in MI:SG2.SP2, Accept Mail. Mail revenue risks predominantly arise at mail acceptance locations; these are where mitigation controls must be implemented to assure mail revenue.

MRA:SG4.SP1 Identify and Assess Mail Revenue Risks

Operational risks to mail revenue are periodically identified and assessed.

Operational risks that can affect mail revenue must be identified and addressed in order to actively manage payment of postage to the USPS. The identification of mail revenue risks forms a baseline from which a continuous risk management process can be established and managed.

The revenue associated with each mailpiece and each mailing is based on the purchased mail services (and other factors such as volume and sortation). The assurance of postage and payment is primarily addressed during the mail acceptance process (refer to MI:SG2.SP2, Accept Mail), given that all postage is prepaid. Mail acceptance personnel (supported by equipment and systems) are responsible for ensuring that all accepted mail meets standards governing mail revenue (as specified in the DMM).

Examples of mail revenue risks are as follows [USPIS 2012, Risk Assessment flow chart]:

- stamps
  - high-quality counterfeit stamps
  - non-reported rejected stamps
  - precanceled stamps bypassing the mail acceptance office at a BMEU
  - stamps purchased with bad checks
  - embezzlement and theft
- metering systems
  - meter tampering, counterfeiting, and duplication
  - software/hardware failures
  - unreadable IBI postage
  - delayed and diverted revenue
  - short-paid mail
  - for PC postage, use of stolen or fraudulent credit cards
- permit imprints
  - induction of bypass mail

- ineligible mail for rate claimed
- lack of visibility of mailpieces for their lifecycle and to payment
- insufficient mail revenue verification processes and tools
- vulnerabilities in technologies that support the assurance of mail revenue

The subpractices included in this practice are generically addressed in goals RISK:SG3 and RISK:SG4 in the Risk Management process area.

Typical Work Products

1. Mail revenue risk statements, with impact valuation
2. List of mail revenue risks, categorized and prioritized

Subpractices

1. Determine the scope of the risk assessment for mail revenue.

   Determining which mailpieces (mail services, types of postage, locations, etc.) to include in regular risk management activities depends on many factors, including the value of the revenue at risk to the USPS.

2. Identify risks to mail revenue.

   Identification of risks to mail revenue requires an examination of all the places where mailpieces are physically accepted (and for some types of mail revenue such as Priority Mail Express, physically delivered). Risks should be identified in this context so that actions to address mail risks are more focused and directed.

3. Analyze risks to mail revenue.
4. Categorize and prioritize risks to mail revenue.
5. Assign a risk disposition to each mail revenue risk.
6. Monitor the risk and the risk strategy on a regular basis to ensure that the risk does not pose additional threat to the payment of mail revenue.
7. Develop a strategy for those risks that the USPS decides to address.

MRA:SG4.SP2 Address Mail Revenue Risks

Identified operational risks to mail revenue are addressed.

Addressing operational risks to mail revenue involves the development of strategies that seek to minimize the risk to an acceptable level. This includes reducing the likelihood of risks to mail revenue, minimizing exposure to these risks, enhancing and developing new plans, procedures, controls, methods and tools for mail revenue verification, and developing recovery plans to address the consequences of realized risk.

The ability to address mail revenue risks requires the development and implementation of risk mitigation plans (which may include the development of new or revision of existing mail revenue controls) and the monitoring of these plans for effectiveness.

Examples of strategies to address mail revenue risks are as follows [USPIS 2012]:

- stamps
  - improvements to the AFCS system
  - review of AFCS rejects
  - additional training
  - analysis of insufficient funds check cases
- metering systems
  - improvements to the TRP system
  - meter vendor reviews
  - vendor meetings to improve readability issues
  - implementation of PASS, which supports standardization, process improvement, and quality control and grants certifications for mailers and vendor systems
- permit imprints
  - full service IMbs to increase the visibility of each mailpiece and payment for it
  - presort investigative tools
  - IMb irregularity reporting
- regularly perform vulnerability scanning, analysis, and resolution on technologies supporting the assurance of mail revenue (refer to the Vulnerability Analysis and Resolution process area)

The subpractices included in this practice are generically addressed in goal RISK:SG5 in the Risk Management process area.

Typical Work Products

1. Plans to address mail revenue risks
2. List of those responsible for addressing and tracking risks
3. Status on plans to address mail revenue risks

Subpractices

1. Develop and implement strategies for all risks that have a “mitigation” or “control” disposition.
2. Validate plans to address mail revenue risks by comparing them to existing strategies for assuring mail revenue.
3. Identify the person or group responsible for each plan and ensure that they have the authority to act and the proper level of skills and training to implement and monitor the plan.
4. Address residual risk.
5. Implement the plans and provide a method to monitor the effectiveness of these plans.
6. Monitor risk status.
7. Collect performance measures on the risk management process.

Mail Revenue Assurance Process Area References

[DMM] *Domestic Mail Manual*, November 2011. Updated online at http://pe.usps.com/text/dmm300/dmm300_landing.htm

[DAR] *Mail Entry & Payment Technology: Commercial Mail Acceptance Transformation. Decision Analysis Report (DAR) Business Case*, Version 0.9, Draft as of 10 February 2012.

[Handbook DM-103] Handbook DM-103 *Official Mail*, December 2004. http://www.apwu.org/sites/apwu/files/resource-files/DM-103%20Official%20Mail%2012-04%20%282.99%20MB%29.pdf

[Handbook DM-109] Handbook DM-109 *Business Mail Acceptance*, March 2010. http://www.apwu.org/sites/apwu/files/resource-files/DM-109%20Business%20Mail%20Acceptance%2003-10%20%283.92%20MB%29.pdf

[Mehravari 2013] "USPIS Introduction to CERT-RMM" course materials, "MRA: Postage Evidence," February 2013; also "Postage Evidence vs. Risks and Systems," 9 January 2013.

[POM] *Postal Operations Manual*, POM Issue 9, July 2002; updated as of December 2011 at http://uspsmanuals.lettercarriernetwork.info/POM9.pdf.

[Stephens 2013] Review comments from Harold Stephens, email, 19 *February* 3013.

[USPIS 2012] USPIS Risk Assessment flow chart, provided by Greg Crabb, January 2012; developed by Michele Culp.

[Wikipedia, 16 March 2012 at 15:04] http://en.wikipedia.org/wiki/Information-Based_Indicia

[Wikipedia, 30 May 2013 at 20:11] http://en.wikipedia.org/wiki/United_States_Postal_Service#Revenue_decline_and_planned_cuts

References

[Allen 2014a] Allen, Julia H.; Crabb, Gregory; Curtis, Pamela D.; Lin, Sam; Mehravari, Nader; & Wilkes, Dawn. *CERT Resilience Management Model Mail-Specific Process Areas: International Mail Transportation, Version 1.0* (CMU/SEI-2014-TN-012). Software Engineering Institute, Carnegie Mellon University, August 2014. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=296395

[Allen 2014b] Allen, Julia H.; Crabb, Gregory; Curtis, Pamela D.; Mehravari, Nader; White, David W. *CERT Resilience Management Model Mail-Specific Process Areas: Mail Induction, Version 1.0* (CMU/SEI-2014-TN-010). Software Engineering Institute, Carnegie Mellon University, August 2014. http://www.sei.cmu.edu/library/asset-view.cfm?assetID=296355

[Caralli 2011] Caralli, Richard A.; Allen, Julia H.; White, David W. *CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience*. Addison-Wesley, 2011. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=30375

[Crabb 2012] Crabb, Gregory. U.S. "Postal Inspection Service Use of the CERT Resilience Management Model" (CERT podcast). Software Engineering Institute, Carnegie Mellon University, August 2012. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=34576

[Crabb 2014] Crabb, Gregory; Allen, Julia H.; Mehravari, Nader; & Curtis, Pamela D. *Improving the Security and Resilience of U.S. Postal Service Mail Products and Services Using the CERT® Resilience Management Mode*l (CMU/SEI-2013-TN-034). Software Engineering Institute, Carnegie Mellon University, January 2014. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=77277

[Joch 2013] Joch, A. "Operational Resilience: Bringing Order to a World of Uncertainty." *Federal Computer Week*, July 8, 2013. http://fcw.com/articles/2013/07/08/exectech-operational-resilience.aspx

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	August 2014	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
CERT Resilience Management Model— Mail-Specific Process Areas: Mail Revenue Assurance (Version 1.0)	FA8721-05-C-0003

6. AUTHOR(S)

Julia H. Allen, Gregory Crabb, Pamela D. Curtis, Nader Mehravari, David W. White

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2014-TN-011

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFLCMC/PZE/Hanscom Enterprise Acquisition Division 20 Schilling Circle Building 1305 Hanscom AFB, MA 01731-2116	n/a

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

Developing and implementing measurable methodologies for improving the security and resilience of a national postal sector directly contribute to protecting public and postal personnel, assets, and revenues. Such methodologies also contribute to the security and resilience of the mode of transport used to carry mail and the protection of the global mail supply chain. Since 2011, the U.S. Postal Inspection Service (USPIS) has collaborated with the CERT® Division at Carnegie Mellon University's Software Engineering Institute (SEI) to improve the resilience of selected U.S. Postal Service (USPS) products and services. The CERT Resilience Management Model (CERT-RMM) and its companion diagnostic methods served as the foundational tool for this collaboration.

This report includes one result of the USPIS/CERT collaboration. It is an extension of CERT-RMM to include a new mail-specific process area for revenue assurance. The purpose is to ensure that the USPS is compensated for all mail that is accepted, transported, and delivered.

14. SUBJECT TERMS	15. NUMBER OF PAGES
CERT-RMM, CERT Resilience Management Model, USPIS	39

16. PRICE CODE

CERT-RMM, USPS, USPIS, resilience, mail specific, mail revenue assurance

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL